

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : William J. Beyda  
Serial No. : 09/668,039  
Filed : September 21, 2000  
Title : PROCESSING ELECTRONIC MESSAGES

Art Unit : 2152  
Examiner : Refai, Ramsey  
Confirmation No.: 9089



BOX APPEAL BRIEF  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

APPEAL BRIEF

I. Real Party in Interest

The real party in interest is Siemens Information and Communications Networks, Inc., a corporation of the State of Delaware having its principal place of business at 900 Broken Sound Blvd., Boca Raton, Florida.

II. Related Appeals and Interferences

Appellant is not aware of any related appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims

Claims 1-5, 14-18, and 29-38, which are the subject of this appeal, are pending.

Claims 1-5, 14-18, and 29-38 stand rejected.

Appellant appeals all rejections of the pending claims 1-5, 14-18, and 29-38.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Box Appeal Brief, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on:

October 10, 2007

Date

(Signature of person mailing papers)

Jeanette L. Taplin

(Typed or printed name of person mailing papers)

**COPY**

#### IV. Status of Amendments

The amendments filed before the final rejection dated April 17, 2007, have been entered and acted upon by the Examiner.

No amendments were filed after the final rejection dated April 17, 2007.

#### V. Summary of Claimed Subject Matter

##### A. Independent claim 1

The aspect of the invention defined in independent claim 1 is an electronic messaging system for filtering electronic messages. The messaging system includes a message server that is operable to receive and transmit electronic messages including electronic mail messages. The message server includes an access restriction filter. The access restriction filter includes a character recognizer that is configured to translate characters in image components of respective ones of electronic messages into computer-readable character representations. The access restriction filter is configured to detect an access restriction notice in the respective ones of the electronic messages by comparing the one or more translated computer-readable character representations respectively produced by the character recognizer to respective representations of one or more access restriction notices stored in memory. The access restriction filter also is configured to respond to the detection of the access restriction notice in accordance with a prescribed transmission policy for handling electronic messages containing the detected access restriction notice.

FIG. 2 shows an embodiment of a universal message server 12 that handles the receipt and transmission of electronic messages from a variety of different message sources 26, including e-mail messages 28, voice mail messages 30, fax messages 32 and video messages 34 (see page 3, lines 21-31, of the specification). The universal message server 12 includes an access restriction filter 40, which includes a message interrogator 42 and one or more prescribed transmission policies 44 specifying the way in which access restriction filter 40 responds to detected access restriction notices (see page 4, lines 7-11, of the specification). The message interrogator 42 includes a character recognizer and is configured to interrogate an electronic message for an access restriction notice (see page 4, lines 13-17, of the specification; FIG. 2).

In accordance with the method shown in FIG. 4, if an electronic message contains one or more still images (FIG. 4, step 68) or video (FIG. 4, block 76), the access restriction filter

40 translates characters in the one or more images or frames of the video into a computer-readable format (e.g., ASCII codes) (see page 5, lines 6-9, of the specification; FIG. 4, steps 70 and 82). Conventional character recognition technology may be used to translate the image data into computer-readable form (see page 5, lines 9-10, of the specification). The translated characters are compared to one or more stored access restriction notices (FIG. 4, steps 72 and 84). If an access restriction notice is detected (see page 5, lines 11-12, of the specification; FIG. 4, step 74), the access restriction filter 40 responds in accordance with one or more prescribed message transmission policies (see page 5, lines 11-13 and 20-22, of the specification; FIG. 4, step 66).

B. Dependent claim 2

Claim 2 depends from claim 1 and recites that “the access restriction filter is configured to detect in respective ones of the electronic messages an access restriction notice indicating ownership of at least a portion of the respective ones of the electronic messages.”

The specification explains that the “electronic message may be interrogated by detecting an ownership notice (e.g., a copyright notice) in the electronic message” (page 2, lines 6-7, of the specification; see also page 4, lines 21-25 and 29-32, and page 5, lines 10-11).

C. Dependent claim 3

Claim 3 depends from claim 2 and recites that “the access restriction filter is configured to detect a copyright notice in respective ones of the electronic messages.”

The specification explains that the “electronic message may be interrogated by detecting an ownership notice (e.g., a copyright notice) in the electronic message” (page 2, lines 6-7, of the specification; see also page 4, lines 21-25 and 29-32, and page 5, lines 10-11).

D. Dependent claim 4

Claim 4 depends from claim 3 and recites that “the access restriction filter is configured to detect the copyright notice by comparing one or more characters in the respective ones of the electronic messages to respective characters of one or more copyright notices stored in memory.”

The specification explains that an “ownership notice may be detected by comparing one or more characters in the electronic message to one or more stored ownership notice representations” (page 2, lines 7-9, of the specification; see also page 4, lines 21-25 and 29-32, and page 5, lines 10-11).

E. Dependent claim 5

Claim 5 depends from claim 3 and recites that “the access restriction filter is configured to detect the copyright notice by comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices.”

The specification explains that an “ownership notice may be detected by interrogating a header component of the electronic message” (page 2, lines 9-10, of the specification; also see page 5, lines 2-6 and 13-17).

F. Dependent claim 33

Claim 33 depends from claim 1 and recites that “at least one of the electronic messages comprises a primary message and at least one attachment, and the access restriction filter is configured to compare characters in the primary message and characters in the at least one attachment to respective characters of the one or more stored access restriction notices.”

The specification explains that an “electronic message may include a primary message and any number of attachments” (page 4, lines 20-21, of the specification). The specification also explains that “if the electronic message contains an email message or a text document, access restriction filter 40 may search the entire email message or text document for a copyright notice symbol (©)” (page 4, lines 30-32, of the specification).

G. Independent claim 14

The aspect of the invention defined in independent claim 14 is a method of filtering electronic messages. In accordance with this inventive method, characters in image components of respective ones of electronic messages are translated into computer-readable character representations. An access restriction notice is detected in the respective ones of the electronic messages by comparing the one or more translated computer-readable character representations to respective representations of one or more access restriction notices stored in memory. The detection of the access restriction notice is responded to in accordance with

a prescribed transmission policy for handling electronic messages containing the detected access restriction notice.

FIG. 2 shows an embodiment of a universal message server 12 that handles the receipt and transmission of electronic messages from a variety of different message sources 26, including e-mail messages 28, voice mail messages 30, fax messages 32 and video messages 34 (see page 3, lines 21-31, of the specification). The universal message server 12 includes an access restriction filter 40, which includes a message interrogator 42 and one or more prescribed transmission policies 44 specifying the way in which access restriction filter 40 responds to detected access restriction notices (see page 4, lines 7-11, of the specification). The message interrogator 42 includes a character recognizer and is configured to interrogate an electronic message for an access restriction notice (see page 4, lines 13-17, of the specification; FIG. 2).

In accordance with the method shown in FIG. 4, if an electronic message contains one or more still images (FIG. 4, step 68) or video (FIG. 4, block 76), the access restriction filter 40 translates characters in the one or more images or frames of the video into a computer-readable format (e.g., ASCII codes) (see page 5, lines 6-9, of the specification; FIG. 4, steps 70 and 82). Conventional character recognition technology may be used to translate the image data into computer-readable form (see page 5, lines 9-10, of the specification). The translated characters are compared to one or more stored access restriction notices (FIG. 4, steps 72 and 84). If an access restriction notice is detected (see page 5, lines 11-12, of the specification; FIG. 4, step 74), the access restriction filter 40 responds in accordance with one or more prescribed message transmission policies (see page 5, lines 11-13 and 20-22, of the specification; FIG. 4, step 66).

#### H. Independent claim 29

The aspect of the invention defined in independent claim 29 is a computer-readable medium comprising computer-readable instructions for causing a computer to perform operations. The computer-readable instructions cause the computer to translate characters in image components of respective ones of electronic messages into computer-readable character representations. The computer-readable instructions cause the computer to detect an access restriction notice in the respective ones of the electronic messages by comparing the one or more translated computer-readable character representations to respective representations of one or more access restriction notices stored in memory. The computer-

readable instructions cause the computer to respond to the detection of the access restriction notice in accordance with a prescribed transmission policy for handling electronic messages containing the detected access restriction notice.

FIG. 2 shows an embodiment of a universal message server 12 that handles the receipt and transmission of electronic messages from a variety of different message sources 26, including e-mail messages 28, voice mail messages 30, fax messages 32 and video messages 34 (see page 3, lines 21-31, of the specification). The specification explains that some embodiments of the universal message server 12 correspond to an Exchange server, which is available from Microsoft Corporation of Redmond, Washington, U.S.A. The universal message server 12 includes an access restriction filter 40, which includes a message interrogator 42 and one or more prescribed transmission policies 44 specifying the way in which access restriction filter 40 responds to detected access restriction notices (see page 4, lines 7-11, of the specification). The message interrogator 42 includes a character recognizer and is configured to interrogate an electronic message for an access restriction notice (see page 4, lines 13-17, of the specification; FIG. 2). The specification explains that the access restriction filter 40 preferably is implemented in a high level procedural or object oriented programming language or in assembly or machine language (see page 6, lines 11-16, of the specification).

In accordance with the method shown in FIG. 4, if an electronic message contains one or more still images (FIG. 4, step 68) or video (FIG. 4, block 76), the access restriction filter 40 translates characters in the one or more images or frames of the video into a computer-readable format (e.g., ASCII codes) (see page 5, lines 6-9, of the specification; FIG. 4, steps 70 and 82). Conventional character recognition technology may be used to translate the image data into computer-readable form (see page 5, lines 9-10, of the specification). The translated characters are compared to one or more stored access restriction notices (FIG. 4, steps 72 and 84). If an access restriction notice is detected (see page 5, lines 11-12, of the specification; FIG. 4, step 74), the access restriction filter 40 responds in accordance with one or more prescribed message transmission policies (see page 5, lines 11-13 and 20-22, of the specification; FIG. 4, step 66).

## VI. Grounds of Rejection to be Reviewed on Appeal

A. Claims 1-5, 14-18, and 29-38 stand rejected under 35 U.S.C. § 103(a) over Fields (U.S. 6,704,797) in view of Sato (U.S. 6,914,691).

## VII. Argument

### **A. Rejection under 35 U.S.C. § 103(a) over Fields (U.S. 6,704,797) in view of Sato (U.S. 6,914,691)**

The Examiner has rejected claims 1-5, 14-18, and 29-38 under 35 U.S.C. § 103(a) over Fields (U.S. 6,704,797) in view of Sato (U.S. 6,914,691).

#### 1. Applicable standards for sustaining a rejection under 35 U.S.C. § 103(a)

"A patent may not be obtained ... if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." 35 U.S.C. §103(a).

In an appeal involving a rejection under 35 U.S.C. § 103, an examiner bears the initial burden of establishing *prima facie* obviousness. See In re Rijckaert, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993). To support a *prima facie* conclusion of obviousness, the prior art must disclose or suggest all the limitations of the claimed invention.<sup>1</sup> See In re Lowry, 32 F.3d 1579, 1582, 32 USPQ2d 1 031, 1034 (Fed. Cir. 1994). If the examiner has established a *prima facie* case of obviousness, the burden of going forward then shifts to the Appellant to overcome the *prima facie* case with argument and/or evidence. Obviousness, is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. This inquiry requires (a) determining the scope and contents of the prior art; (b) ascertaining the differences between the prior art and the claims in issue; (c) resolving the level of ordinary skill in the pertinent art; and (d) evaluating evidence of secondary consideration. See KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 2 (U.S. Apr. 30, 2007) (citing Graham v. John Deere, 383 U.S. 1, 17-18, 148 USPQ 459, 467 (1966)). If all claim limitations are found in a number of prior art references, the fact finder must determine

---

<sup>1</sup> The U.S. Patent and Trademark Office has set forth the following definition of the requirements for establishing a *prima facie* case of unpatentability (37 CFR § 1.56(b)(ii):

A *prima facie* case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

whether there was an apparent reason to combine the known elements in the fashion claimed. See KSR, slip op. at 14. This analysis should be made explicit. KSR, slip op at 14 (citing In re Kahn, 441 F. 3d 977, 988 (CA Fed. 2006): “[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”).

## 2. Overview of Fields' disclosure

Fields discloses a web sever 20 that includes an access manager 34 that handles client web browser requests for a protected original image or for web pages containing the protected original image. The access manager 34 handles the client web browser requests in accordance with a server-based policy defined by one or more rules for selectively distributing different versions of the original image, if any (see, e.g., col. 2, lines 36-58, col. 4, lines 36-43, and col. 6, lines 2-7; FIG. 2).

In accordance with Fields' disclosure, different versions of an image are stored at the server 20 (see col. 4, lines 34-35). Exemplary types of image versions include a low-resolution version, an outdated version, a grayscale version, a cropped version, and a symbol-overlaid version (see col. 6, lines 33-57; FIG. 4). Each version of the image is associated with a respective client-specific access criterion that is defined in terms of client-specific data (see col. 4, lines 35-36). FIG. 5 shows a user interface that allows a user to associate each image version with a respective client-specific access criterion.

Exemplary types of client-specific access criteria include the identity of the referring page, the client machine IP address, an ISP identity, a user identifier such as a cookie, and the existence of a user authentication (see col. 2, line 65 - col. 3, line 3). Exemplary types of policy rules that the access manager 34 might enforce include the following (col. 2, lines 48-58):

Thus, for example, a given policy may include a rule that a given image is not distributed from the server to any referring pages outside of a given domain. Another rule may restrict distribution to a modified version of an image, e.g., a version that is overlaid with a company logo or watermark, to any client machine that is not on a permitted list of IP addresses. Yet another rule may restrict distribution to a low resolution version of the image to any referring page that is within a given third party domain. Of course, the above examples are merely exemplary.



When a client web browser request requiring the delivery of a protected image is received by the web server 20, the access manager 34 evaluates the one or more client-specific access criteria in the rules against the client-specific data in the client web browser request (see, e.g., col. 2, lines 41-44, and col. 5, lines 26-29). The access manager 34 serves the version of the protected image that is associated with the client-specific access criterion that matches the client-specific data in the request, if any (see, e.g., col. 2, lines 44-58, and col. 4, lines 34-43).

### 3. Overview of Sato's disclosure

Sato discloses an image processing system that includes a host computer 101, a print controller 102, and a printer 103 (see col. 2, lines 61-67; FIG. 1). The host computer 101 converts image data into page description language (PDL) data (see col. 3, lines 3-6). The print controller 102 translates the PDL data into raster image data (see col. 3, lines 7-12). The printer 103 prints the raster image data received from the print controller 102 onto a manuscript (see col. 2, line 66 - col. 3, line 2).

The print controller 102 includes a copyright-information detecting circuit 105 that executes a pattern matching algorithm or a character recognition algorithm to detect the presence of a copyright indication (e.g., a mark, bar code, or character string) in the raster image data that is produced by the print controller 102 (see col. 8, lines 1 - 34). In some embodiments, if the detection circuit 105 detects the presence of the copyright indication, the image data is not sent to the image forming device 103 for printing (see col. 7, lines 35-45).

### 4. Independent claim 1

#### a. Introduction

Claim 1 recites:

1. An electronic messaging system for filtering electronic messages, comprising  
a message server operable to receive and transmit electronic messages including electronic mail messages, the message server comprising an access restriction filter comprising a character recognizer configured to translate characters in image components of respective ones of electronic messages into computer-readable character representations,

wherein the access restriction filter is configured to detect an access restriction notice in the respective ones of the electronic messages by comparing the one or more translated computer-readable character representations respectively produced by the character recognizer to respective representations of one or more access restriction notices stored in memory, the access restriction filter being additionally configured to respond to the detection of the access restriction notice in accordance with a prescribed transmission policy for handling electronic messages containing the detected access restriction notice.

For the reasons explained in detail below, the rejection of claim 1 under 35 U.S.C. § 103(a) over Fields in view of Sato should be withdrawn because (i) the Examiner has not established a *prima facie* case of obviousness, and (ii) one skilled in the art would not have had any apparent reason to combine the references in the manner proposed by the Examiner.

b. The Examiner's position

In support of the rejection of independent claim 1, the Examiner has stated that (see § 4, pages 4-5 of the final Office action; paragraph numbers and emphasis added):

- (1) As per claim 1, Fields et al teach an electronic messaging system for filtering electronic messages, comprising
- (2) a message server operable to receive and transmit electronic messages including electronic mail messages (column 3, line 65), the message server comprising an access restriction filter (column 2, lines 40-58, column 6, lines 52-54);
- (3) wherein the access restriction filter is configured to detect an access restriction notice in the respective ones of the electronic messages, and, the access restriction filter being additionally configured to respond to the detection of the access restriction notice in accordance with a prescribed policy for handling electronic messages containing the detected access restriction notice (column 2, line 35 - column 3, line 15).
- (4) Fields et al fail to teach the access restriction filter comprising a character recognizer configured to translate characters in image components of respective ones of electronic messages into computer-readable character representations and comparing the one or more translated computer readable character representations respectively produced by the character recognizer to respective representations of one or more access restriction notices stored-in memory. However, Sato teach a detection process for detecting copyright restriction characters on images and executes pattern matching with characters stored

in memory to impose stored restriction policies, such as prevent copying of the image (column 8, lines 9-34). It would have been obvious to one of the ordinary skill in the art to combine the teachings of Fields et al and Sato because doing so would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image.

c. Applicant's rebuttal to Examiner's position

i. The Examiner has not established a *prima facie* case of obviousness

The rejection of claim 1 under 35 U.S.C. § 103(a) over Fields in view of Sato should be withdrawn because the Examiner has not established a *prima facie* case of obviousness. As explained above, to support a *prima facie* conclusion of obviousness, the prior art must disclose or suggest all the limitations of the claimed invention. See *In re Lowry*, 32 F.3d 1579, 1582, 32 USPQ2d 1 031, 1034 (Fed. Cir. 1994). For the reasons explained in detail below, however, Fields and Sato, taken either alone or in any permissible combination, do not disclose or suggest all the elements of the claimed invention.

The Examiner's position in numbered paragraphs (1)-(3) quoted above is premised on the correspondence between Fields' access manager 34 and the access restriction filter recited in claim 1. In accordance with Fields' disclosure, the access manager 34 evaluates the one or more client-specific access criteria in the policy rules against the client-specific data in the client web browser request (see, e.g., col. 2, lines 41-44, and col. 5, lines 26-29) and serves the version of the protected image that is associated with the client-specific access criterion that matches the client-specific data in the request, if any (see, e.g., col. 2, lines 44-58, and col. 4, lines 34-43). Thus, the Examiner has taken the position that a client web browser request constitutes an electronic message in which the access manager 34 "is configured to detect an access restriction notice," as recited in claim 1. Fields' access manager 34, however, does not detect an access restriction notice in such a client web browser request. Instead, the access manager 34 only compares the client-specific data in a given client request to the policy rules criteria that are stored on the server (see, e.g., col. 5, lines 26-30). The client-specific data includes "an identity of a referring page (i.e. the page from which the link to the server was selected), a client machine IP address, the identity of a third party service provider (e.g., an ISP) that provides Internet service to the client, the existence (or lack thereof) of a user authentication, a user identifier such as a cookie, or other such data" (col. 4, lines 25-32). None of the client-specific data constitutes an "access restriction notice" within

the ordinary and accustomed meaning of the term. Consequently, Fields' access manager 34 is not configured to detect "an access restriction notice" in the web browser requests that are received from the client 10.

The Examiner has responded to this point as follows (see § 1, page 2, response to "Argument A"):

In response, the Examiner respectfully disagrees. Fields teaches a method to protect images via a server-based policy (column 2, lines 37-38). When a client requests an image or a web page containing the image, the method parses the request and examines the image. A rule for the image is evaluated against client specific data. If the condition is satisfied an image restriction is imposed. (column 2, line 36-column 3, line 15, column 7, lines 40-67). Therefore, Fields meets the scope of the claimed access restriction filter, which is configured to detect an access restriction notice in the respective ones of the electronic messages. Rejection is maintained.

The client-specific data against which the policy rules are evaluated do not constitute "an access restriction notice" under any reasonable interpretation of the term. The only types of client-specific data disclosed by Fields are "an identity of a referring page (i.e. the page from which the link to the server was selected), a client machine IP address, the identity of a third party service provider (e.g., an ISP) that provides Internet service to the client, the existence (or lack thereof) of a user authentication, a user identifier such as a cookie, or other such data" (col. 4, lines 25-32). There is no reasonable basis for the Examiner's assumption that the ordinary and accustomed meaning of the term "access restriction notice" encompasses any of the types of client-specific data disclosed in Fields.

Sato does not make-up for the failure of Fields to disclose or suggest an "access restriction filter is configured to detect an access restriction notice in the respective ones of the electronic messages," as recited in claim 1. Indeed, Sato does not disclose or suggest anything about detecting access restrictions notices in electronic messages of the type recited in claim 1.

Thus, neither Fields nor Sato discloses or suggests an "access restriction filter is configured to detect an access restriction notice in the respective ones of the electronic messages," as recited in claim 1. The Examiner has not pointed to any suggestion or motivation in the knowledge that was generally available to one of ordinary skill in the art that makes up for the failure of Fields and Sato to disclose or suggest this element of claim 1.

Therefore, the rationale given by the Examiner in support of the rejection of claim 1 does not show that the combination of Fields and Sato includes an "access restriction filter is configured to detect an access restriction notice in the respective ones of the electronic messages," as recited in claim 1. For at least this reason, the Examiner has not established a *prima facie* case of obviousness and the rejection of claim 1 under 35 U.S.C. § 103(a) over Fields in view of Sato should be withdrawn.

The Examiner's rejection of claim 1 also should be withdrawn for the following additional reason.

ii. One skilled in the art would not have had any apparent reason to combine the references in the manner proposed by the Examiner

As explained in detail below, the Examiner's rationale in support of the rejection of claim 1 amounts to no more than a conclusory statement that does not have any rational underpinning that supports a rejection under 35 U.S.C. § 103. See KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 14 (U.S. Apr. 30, 2007) (citing In re Kahn, 441 F. 3d 977, 988 (CA Fed. 2006): "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

The Examiner has acknowledged that Fields "fail to teach the access restriction filter comprising a character recognizer configured to translate characters in image components of respective ones of electronic messages into computer-readable character representations and comparing the one or more translated computer readable character representations respectively produced by the character recognizer to respective representations of one or more access restriction notices stored-in memory" (see paragraph (4) quoted above, and § 4, page 5, lines 3-8, of the final Office action). In an effort to make-up for this failure, the Examiner has stated that (page 5, lines 8-13, of the final Office action; emphasis added):

However, Sato teach a detection process for detecting copyright restriction characters on images and executes pattern matching with characters stored in memory to impose stored restriction policies, such as prevent copying of the image (column 8, lines 9-34). It would have been obvious to one of the ordinary skill in the art to combine the teachings of Fields et al and Sato because doing so would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image.

Contrary to the Examiner's statement, however, one skilled in the art at the time the invention was made would not have been led to combine the teachings of Fields and Sato to arrive at the inventive electronic messaging system recited in claim 1.

First, Fields does not detect access restriction notices in the client web browser requests, which constitute the electronic messages recited in claim 1 in accordance with the rationale provided by the Examiner in support of the rejection of claim 1. Sato discloses a copyright-information detecting circuit 105 that executes a pattern matching algorithm or a character recognition algorithm to detect the presence of a copyright indication in the raster image data that is produced by the print controller 102. This disclosure, however, does not disclose or suggest anything that would have led one skilled in the art to detect access restriction notices in client web browser requests of the type handled by Fields' access manager 34. Indeed, such web browser requests do not contain any raster image data that could be processed by Sato's copyright-information detecting circuit 105. Therefore, the Examiner has not pointed to any suggestion or motivation, either in Fields, Sato, or in the knowledge generally available that would have led one skilled in the art to modify or combine the teachings of Fields and Sato in a way that would result in the inventive subject matter defined in claim 1.

Second, the Examiner's conclusion of obviousness is based on the contention that one skilled in the art would have found it obvious "to combine the teachings of Fields et al and Sato." One skilled in the art at the time the invention was made, however, would not have been motivated to combine the teachings of Fields and Sato in the manner proposed by the Examiner because such a combination would not serve any useful purpose whatsoever. As explained above, the client requests for images or web pages containing images do not contain the images whose access is being controlled by Fields' access manager 34. Indeed, these client requests would not be made if they already contained the images. Therefore, one skilled in the art would not have any reason whatsoever to use Sato's detection circuit 105 to detect the presence of a copyright indication in the client requests that are received by Fields' access manager 34.

The Examiner has not pointed to any suggestion or motivation, either in the cited references or in the knowledge generally available, which would have led one skilled in the art to make-up for the fact that the client requests handled by Fields' access manager 34 do not include the images whose access is being controlled by Fields' access manager 34 nor any raster image data for that matter. In fact, the Examiner has not explained his proposed

combination of the teachings of Fields and Sato with any level of specificity whatsoever, much less in a way that shows how the proposed combination results in the inventive subject matter defined by independent claim 1. The only hint of the Examiner's vision of the combination of the reference teachings is contained in the following statement (see page 5, lines 12-13 of the final Office action):

... because doing so would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image.

This statement, however, does not explain how Sato's copyright-information detecting circuit 305 would have been combined with Platt's media object management system to arrive at the inventive subject matter defined in claim 1. For example, the Examiner has not explained how Sato's detecting circuit 105, which is designed to apply pattern matching or character recognition techniques to raster image data, could be applied to web browser requests that do not contain such raster image data. Clearly, it is not possible to say that it would have been obvious to one skilled in the art to combine the teachings of Fields and Sato without specifying the details of that proposed combination. In effect, without specifying the details of the proposed combination of the reference teachings that is envisioned by the Examiner, the Examiner's basis for rejecting claim 1 amounts to no more than an impermissible conclusory statement that cannot support a rejection under 35 U.S.C. § 103. See KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 14 (U.S. Apr. 30, 2007). In fact, the inability of the Examiner to articulate the details of his proposed combination evidences the unobviousness of the Examiner's proposed combination.

Furthermore, the only support given by the Examiner for his conclusion that it would have been obvious to combine the teachings of Platt and Borman is "because doing so would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image" (see page 5, lines 12-13 of the final Office action). However, the possibility that the combined teaching "would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image" does not constitute a showing of a suggestion or a motivation, either in the cited references themselves or in the knowledge generally available, that would have given one skilled in the art any apparent reason to modify the references or to combine the reference teachings, especially in light of the fact that the client requests handled by Fields' access manager 34 do not include any raster image

data, much less do they contain the images whose access is being controlled by Fields' access manager 34.

In addition, there is no basis whatsoever for the Examiner's conclusion that a combination of Fields and Sato "would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image." If the Examiner's persists with his reliance on this rationale in support of the rejection of claim 1, Appellant asks the Examiner to explain how the combination of Fields and Sato "would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image." In this regard, Appellant asks the Examiner to explain how the detection of copyright-information in non-existent image data in client web browser requests "would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image" when the client web browser requests do not contain the protected images.

For the reasons explained above, the Examiner's rationale in support of his proposed combination of Fields and Sato amounts to no more than an impermissible conclusory statement, which cannot establish that one skilled in the art would have had any apparent reason to combine Fields and Sato in the manner proposed by the Examiner. For at least these additional reasons, the rejection of claim 1 under 35 U.S.C. § 103(a) over Fields in view of Sato should be withdrawn. See In re Kahn, 441 F. 3d 977, 988 (CA Fed. 2006) ("[R]jections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

In the final Office action, the Examiner did not respond substantively to the points raised above. Instead, the Examiner merely re-stated the same rationale, which is quoted above and was given by the Examiner in § 4 on pages 2-3 of the non-final Office action dated September 1, 2006 (see § 1, page 3, lines 4-18, of the final Office action).

##### 5. Claims 2-5, 30, and 33-35

Each of claims 2-5, 30, and 33-35 incorporates the features of independent claim 1 and therefore is patentable over Fields and Sato for at least the same reasons explained above. The Examiner's rejections of these claims also should be withdrawn for the following additional reasons.



a. Claim 2

Claim 2 depends from claim 1 and recites that “the access restriction filter is configured to detect in respective ones of the electronic messages an access restriction notice indicating ownership of at least a portion of the respective ones of the electronic messages.”

In support of the rejection of claim 2, the Examiner has stated that “Fields et al teach wherein the access restriction filter is configured to detect in respective ones of the electronic messages an access restriction notice indicating ownership of at least a portion of the respective ones of the electronic message (column 2, lines 35-60).”

Col. 2, lines 35-60, of Fields does not support the Examiner's contention that Fields teaches that “the access restriction filter is configured to detect in respective ones of the electronic messages an access restriction notice indicating ownership of at least a portion of the respective ones of the electronic message.” Fields does not even hint that the access manager 34 detects an access restriction notice indicating ownership of at least a portion of a client request.

The Examiner has responded to this point as follows (see § 1, page 4, lines 5-7, of the final Office action):

In response, the Examiner respectfully disagrees. The detecting of images that contain watermark or company logos indicate ownership of an image (column 2, lines 51-53, column 5, lines 40-67).

In col. 2, lines 51-53, and col. 5, lines 40-67, Fields discloses an example of a policy rule that restricts distribution of a protected to a modified version of the image that is overlaid with a company logo or watermark. This disclosure relates to the type of image that is served in response to the client web browser request. This disclosure does not change the fact that the access manager 34 evaluates client-specific data in the request against client-specific access criteria specified in the policy rule; the access manager 34 does not detect anything whatsoever in the protected images or the image versions derived from the protected images.

b. Claim 3

Claim 3 depends from claim 2 and recites that “the access restriction filter is configured to detect a copyright notice in respective ones of the electronic messages.”

In support of the rejection of claim 3, the Examiner has stated that "Fields et al teach wherein the access restriction filter is configured to detect a copyright notice in respective ones of the electronic message (column 1, lines 35-41, column 6, lines 50-54)."

The disclosure in col. 1, lines 35-41, and col. 6, lines 50-54, does not support the Examiner's contention that Fields teaches that "the access restriction filter is configured to detect a copyright notice in respective ones of the electronic message." The description of the rights of copyright owners in col. 1, lines 35-41, does not constitute a teaching that the access manager 34 is configured to detect a copyright notice in a client request for an image or a web page containing an image. In addition, in col. 6, lines 50-54, Fields discloses that a user may create a version of an image that includes a symbol overlay, such as a copyright symbol overlay. Contrary to the Examiner's statement, however, this disclosure does not constitute a teaching that the access manager 34 is configured to detect a copyright notice in a client request for an image or a web page containing an image.

The Examiner did not respond to this point in the final Office action.

c. Claim 4

Claim 4 depends from claim 3 and recites that "the access restriction filter is configured to detect the copyright notice by comparing one or more characters in the respective ones of the electronic messages to respective characters of one or more copyright notices stored in memory."

In support of the rejection of claim 4, the Examiner has stated that "Fields et al teach wherein the access restriction filter is configured to detect the copyright notice by comparing one or more characters in the respective ones of electronic messages to respective characters of one or more copyright notices stored in memory (column 2, line 35-column 3, line 15)."

The disclosure on col. 2, line 35 - col. 3, line 15, does not support the Examiner's contention that Fields teaches that "the access restriction filter is configured to detect the copyright notice by comparing one or more characters in the respective ones of the electronic messages to respective characters of one or more copyright notices stored in memory." Indeed, the cited disclosure does not teach anything about detecting copyright notices in client requests for images or web pages containing images, much less anything about comparing one or more characters in the respective ones of the electronic messages to respective characters of one or more copyright notices stored in memory.

The Examiner did not respond to this point in the final Office action.

d. Claim 5

Claim 5 depends from claim 3 and recites that "the access restriction filter is configured to detect the copyright notice by comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices."

In support of the rejection of claim 4, the Examiner has stated that "Fields et al teach wherein the access restriction filter is configured to detect the copyright notice by comparing characters in header component of the respective ones of electronic messages with respective characters of the one or more stored copyright notices (column 4, lines 44-67)."

The disclosure on col. 4, line 44-67, does not support the Examiner's contention that Fields teaches that "the access restriction filter is configured to detect the copyright notice by comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices." Indeed, the cited disclosure does not teach anything about detecting copyright notices in client requests for images or web pages containing images, much less anything about comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices. Instead, this disclosure merely describes how an image version is served by the access manager 34 in response to a client request.

The Examiner did not respond to this point in the final Office action.

e. Claim 33

Claim 33 depends from claim 1 and recites that "at least one of the electronic messages comprises a primary message and at least one attachment, and the access restriction filter is configured to compare characters in the primary message and characters in the at least one attachment to respective characters of the one or more stored access restriction notices."

In support of the rejection of claim 4, the Examiner has stated that "Fields et al teach wherein at least one of the electronic message comprises a primary message and at least one attachment, and the access restriction filter is configured to compare characters in the primary message and characters in the at least one attachment to respective characters of the one or more stored access restriction notices (column 4, lines 34-39)."

The disclosure on col. 4, line 34-39, does not support the Examiner's contention that Fields teaches that "at least one of the electronic messages comprises a primary message and

at least one attachment, and the access restriction filter is configured to compare characters in the primary message and characters in the at least one attachment to respective characters of the one or more stored access restriction notices." Indeed, the cited disclosure does not teach anything that would have led one skilled in the art to believe that any of the client requests includes a primary message and at least one attachment. Instead, this disclosure teaches that a set of image versions are stored at the server and that each image version is associated with distribution criteria.

The Examiner did not respond to this point in the final Office action.

6. Independent claim 14

Independent claim 14 recites features that essentially track the pertinent features of independent claim 1 discussed above. Therefore, claim 14 is patentable over Fields and Sato for at least the same reasons explained above in connection with independent claim 1.

7. Dependent claims 15-18 and 31

Each of claims 15-18 and 31 incorporates the features of independent claim 14 and therefore is patentable over Fields and Sato for at least the same reasons explained above.

Claims 15-18 also are patentable over Fields and Sato for the same additional reasons explained above in connection with claims 2-5, respectively.

8. Independent claim 29

Independent claim 29 recites features that essentially track the pertinent features of independent claim 1 discussed above. Therefore, claim 29 is patentable over Fields and Sato for at least the same reasons explained above in connection with independent claim 1.

9. Dependent claim 32

Claim 32 incorporates the features of independent claim 29 and therefore is patentable over Fields and Sato for at least the same reasons explained above.

VIII. Conclusion

For the reasons explained above, all of the pending claims are now in condition for allowance and should be allowed.

This Appeal Brief is submitted in TRIPLICATE.

Applicant : William J. Beyda  
Serial No. : 09/668,039  
Filed : September 21, 2000

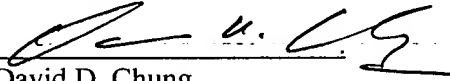
Attorney's Docket No.: 2000P07906US02  
Appeal Brief dated October 10, 2007  
Reply to Final Action dated April 17, 2007

Charge any excess fees or apply any credits to Deposit Account No. 19-2179.

Date: 10 Oct. 07

SIEMENS CORPORATION  
**Customer Number: 28524**  
Intellectual Property Department  
170 Wood Avenue South  
Iselin, New Jersey 08830

Respectfully submitted,

By:   
David D. Chung  
Registration No. 38,409  
Attorney for Applicants  
**Direct Dial: 408-492-5336**  
Dept. Fax: 408-492-3122

CLAIMS APPENDIX

The claims that are the subject of Appeal are presented below.

Claim 1 (previously presented): An electronic messaging system for filtering electronic messages, comprising

a message server operable to receive and transmit electronic messages including electronic mail messages, the message server comprising an access restriction filter comprising a character recognizer configured to translate characters in image components of respective ones of electronic messages into computer-readable character representations,

wherein the access restriction filter is configured to detect an access restriction notice in the respective ones of the electronic messages by comparing the one or more translated computer-readable character representations respectively produced by the character recognizer to respective representations of one or more access restriction notices stored in memory, the access restriction filter being additionally configured to respond to the detection of the access restriction notice in accordance with a prescribed transmission policy for handling electronic messages containing the detected access restriction notice.

Claim 2 (previously presented): The system of claim 1, wherein the access restriction filter is configured to detect in respective ones of the electronic messages an access restriction notice indicating ownership of at least a portion of the respective ones of the electronic messages.

Claim 3 (previously presented): The system of claim 2, wherein the access restriction filter is configured to detect a copyright notice in respective ones of the electronic messages.

Claim 4 (previously presented): The system of claim 3, wherein the access restriction filter is configured to detect the copyright notice by comparing one or more characters in the respective ones of the electronic messages to respective characters of one or more copyright notices stored in memory.

Claim 5 (previously presented): The system of claim 3, wherein the access restriction filter is configured to detect the copyright notice by comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices.

Claims 6-13 (canceled)

Claim 14 (previously presented): A method of filtering electronic messages, comprising:

translating characters in image components of respective ones of electronic messages into computer-readable character representations;

detecting an access restriction notice in the respective ones of the electronic messages by comparing the one or more translated computer-readable character representations to respective representations of one or more access restriction notices stored in memory; and

responding to the detection of the access restriction notice in accordance with a prescribed transmission policy for handling electronic messages containing the detected access restriction notice.

Applicant : William J. Beyda  
Serial No. : 09/668,039  
Filed : September 21, 2000

Attorney's Docket No.: 2000P07906US02  
Appeal Brief dated October 10, 2007  
Reply to Final Action dated April 17, 2007

Claim 15 (previously presented): The method of claim 14, wherein the detecting comprises detecting in respective ones of the electronic message an access restriction notice indicating ownership of at least a portion of the respective ones of the electronic messages.

Claim 16 (previously presented): The method of claim 15, wherein the detecting comprises detecting a copyright notice in respective ones of the electronic messages.

Claim 17 (previously presented): The method of claim 16, wherein the detecting comprises comparing one or more characters in the respective ones of the electronic messages to respective characters of one or more copyright notices stored in memory.

Claim 18 (previously presented): The method of claim 16, wherein the detecting comprises comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices.

Claims 19-28 (canceled)

Claim 29 (previously presented): A computer-readable medium comprising computer-readable instructions for causing a computer to perform operations comprising:  
translating characters in image components of respective ones of electronic messages into computer-readable character representations;  
detecting an access restriction notice in the respective ones of the electronic messages by comparing the one or more translated computer-readable character representations to respective representations of one or more access restriction notices stored in memory; and



responding to the detection of the access restriction notice in accordance with a prescribed transmission policy for handling electronic messages containing the detected access restriction notice.

Claim 30 (previously presented): The system of claim 1, wherein the access restriction filter is configured to detect at least one of the following access restriction notices in the electronic messages: a "confidential" notice, an "internal use only" notice, an "attorney-client privileged" notice, and an "attorney work product" notice.

Claim 31 (previously presented): The method of claim 14, wherein the detecting comprises detecting at least one of the following access restriction notices in the electronic messages: a "confidential" notice, an "internal use only" notice, an "attorney-client privileged" notice, and an "attorney work product" notice.

Claim 32 (previously presented): The computer-readable medium of claim 29, wherein said code provides instructions for detecting in the electronic messages at least one of a "copyright" notice, a "confidential" notice, an "internal use only" notice, an "attorney-client privileged" notice, and an "attorney work product" notice.

Claim 33 (previously presented): The system of claim 1, wherein at least one of the electronic messages comprises a primary message and at least one attachment, and the access restriction filter is configured to compare characters in the primary message and characters in the at least one attachment to respective characters of the one or more stored access restriction notices.

Applicant : William J. Beyda  
Serial No. : 09/668,039  
Filed : September 21, 2000

Attorney's Docket No.: 2000P07906US02  
Appeal Brief dated October 10, 2007  
Reply to Final Action dated April 17, 2007

Claim 34 (previously presented): The system of claim 1, wherein the access restriction filter is configured to trigger display of a report to a user in response to the detection of the access restriction notice.

Claim 35 (previously presented): The system of claim 34, wherein the access restriction filter is configured to trigger display to a user a message reporting that a corresponding one of the electronic messages cannot be transmitted because of the detection of the access restriction.

Claim 36 (previously presented): The method of claim 14, wherein the responding comprises displaying a report to a user in response to the detection of the access restriction notice.

Claim 37 (previously presented): The method of claim 36, wherein the responding comprises displaying to a user a message reporting that a corresponding one of the electronic messages cannot be transmitted because of the detection of the access restriction.

Claim 38 (previously presented): The system of claim 1, wherein character recognizer configured to translate characters in image components of respective ones of electronic mail messages into computer-readable character representations, and the access restriction filter is configured to detect an access restriction notice in the respective ones of the electronic mail messages by comparing the one or more translated computer-readable character representations respectively produced by the character recognizer to respective representations of one or more access restriction notices stored in memory.

Applicant : William J. Beyda  
Serial No. : 09/668,039  
Filed : September 21, 2000

Attorney's Docket No.: 2000P07906US02  
Appeal Brief dated October 10, 2007  
Reply to Final Action dated April 17, 2007

### EVIDENCE APPENDIX

There is no evidence submitted pursuant to 37 CFR §§ 1.130, 1.131, or 1.132 or any other evidence entered by the Examiner and relied upon by Appellant in the pending appeal. Therefore, no copies are required under 37 CFR § 41.37(c)(1)(ix) in the pending appeal.

Applicant : William J. Beyda  
Serial No. : 09/668,039  
Filed : September 21, 2000

Attorney's Docket No.: 2000P07906US02  
Appeal Brief dated October 10, 2007  
Reply to Final Action dated April 17, 2007

RELATED PROCEEDINGS APPENDIX

Appellant is not aware of any decisions rendered by a court or the Board that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal. Therefore, no copies are required under 37 CFR § 41.37(c)(1)(x) in the pending appeal.